October 2008

Security Testing with CORE IMPACT

Anthony Alves, Senior Sales Engineer

Situation Analysis – The Threat Environment

- **Threats are …**
  - increasingly sophisticated
  - well-funded and staffed
  - complex in breadth and depth
- **IT environments are …**
  - increasingly dynamic and interconnected
  - incorporating new technologies (i.e., potential threat vectors)
  - becoming mission-critical for revenue and customer service
- **Security spending continues to increase exponentially, however:**
  - traditional security strategies are imperfect and siloed
  - organizations can't measure overall security effectiveness or efficiently mitigate risk
- **Organizations can't just keep throwing money at point solutions.**
  - Need to measure what's working, what's not and what to do about it.

Organizational Challenges

- **The Problem:**
  - Security incidents continue to occur despite widespread deployment of point defensive technologies and security assurance solutions.
  - Point solutions can't effectively communicate with each other about real risk.
  - Threats are complex – A single threat can compromise multiple vulnerable layers of IT.
  - Stopping with the deployment of point defensive and testing solutions = an incomplete vulnerability management process
    - » results in information overload
    - » does not account for complex, multistaged threats
- **The Result:**
  - Limited visibility into the overall security posture
  - Lack of actionable data to assist with mitigating risk
- **What's Missing:**
  - To truly understand threat readiness, you need to test your security in a comprehensive way, using solutions that account for real-world threat behavior.

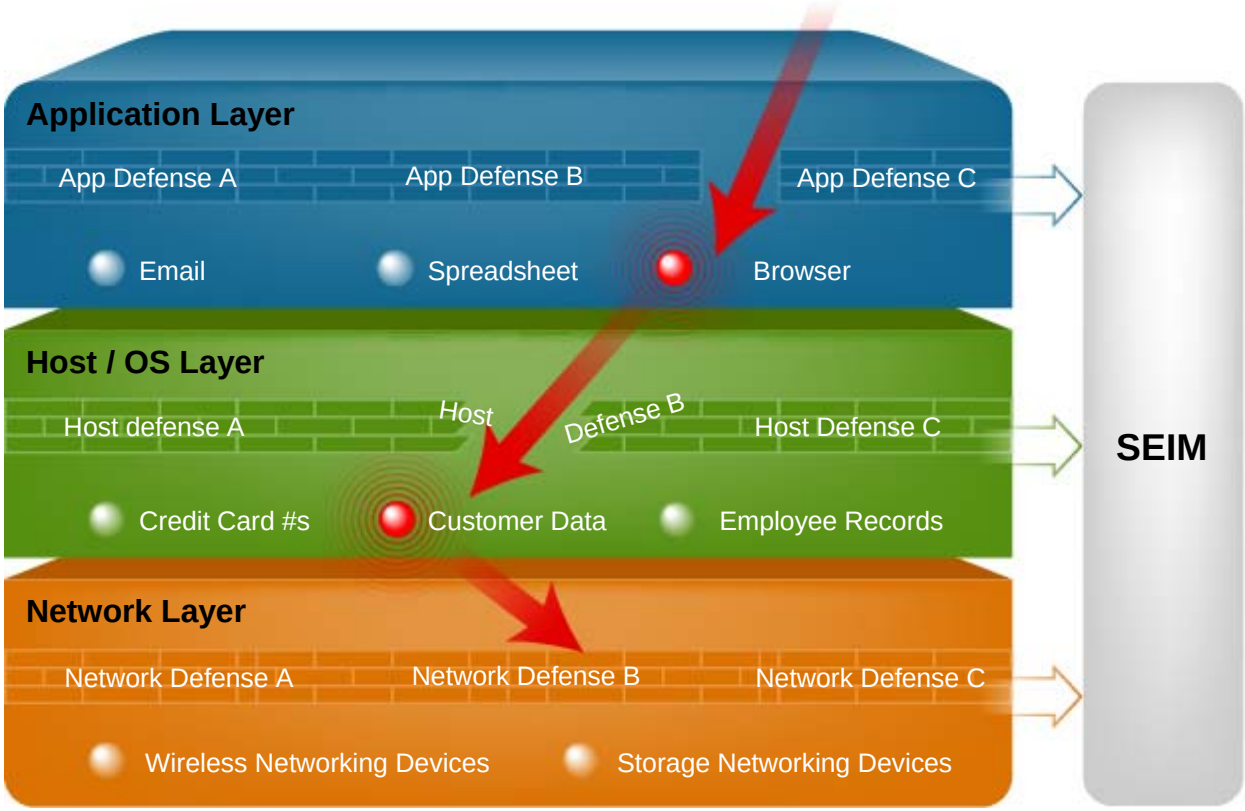
Real-World Attack Behavior

Cybercriminals are still finding their way around, and through, point security defenses.

New attack paths

Point defense weaknesses

Multistaged threats that move across systems and IT layers to threaten critical backend assets



How do you know what's working, what's not, and what to do about it?

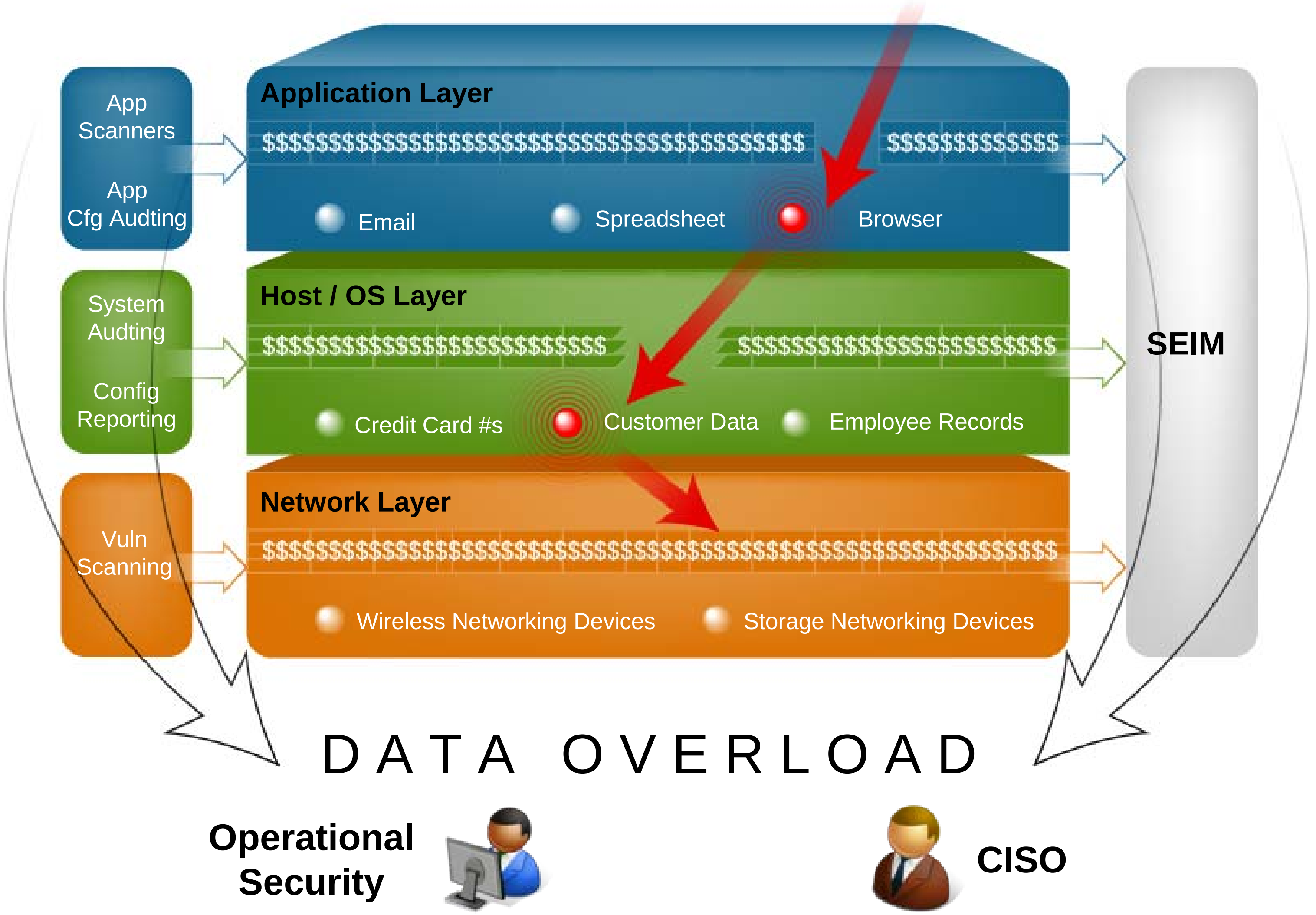
Security Assurance: “Testing in Layers”

www.coresecurity.com

Point testing data
+ Defensive app logs
+ SEIM data

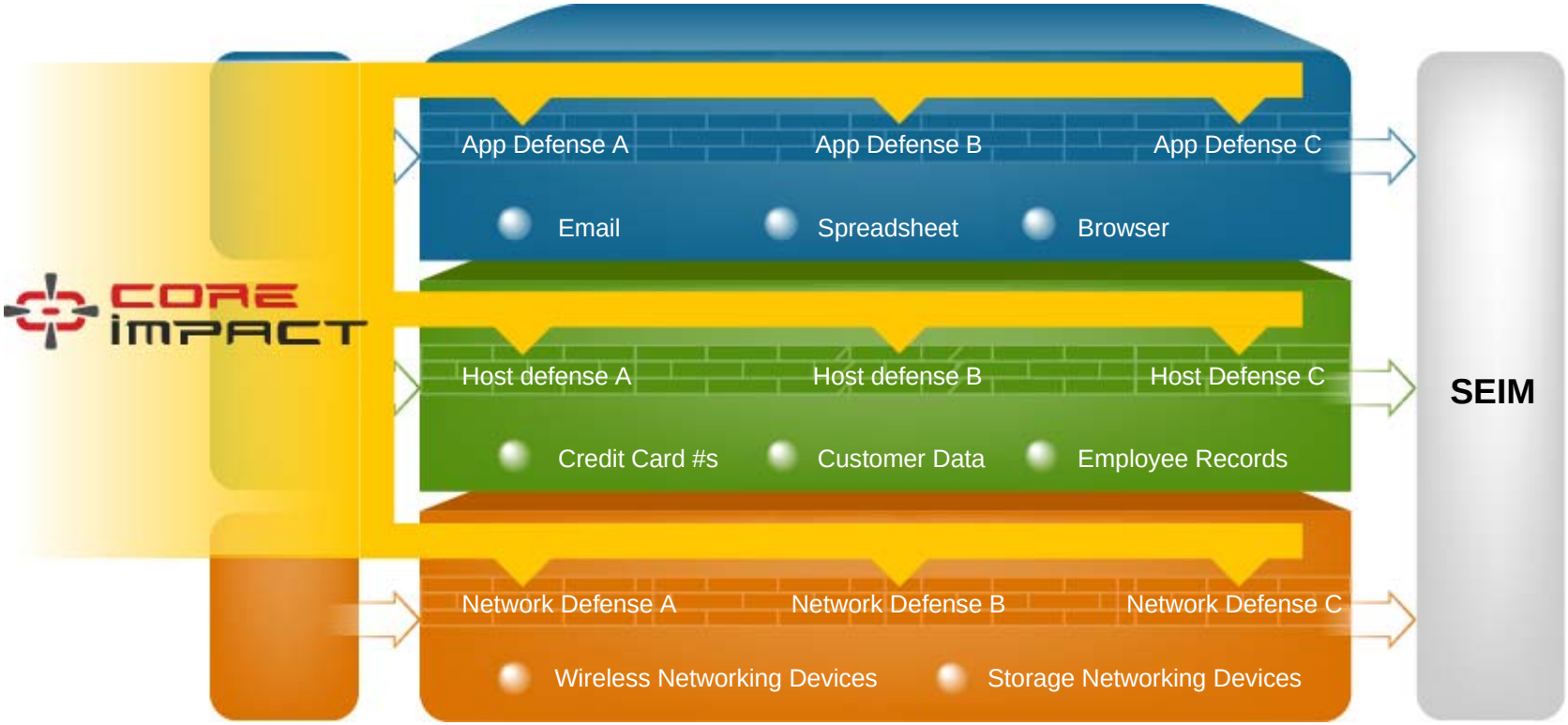
= **Data Overload**

Typical reaction: spend more on defenses, without clear insights into critical risks (i.e., where defensive resources are actually needed).



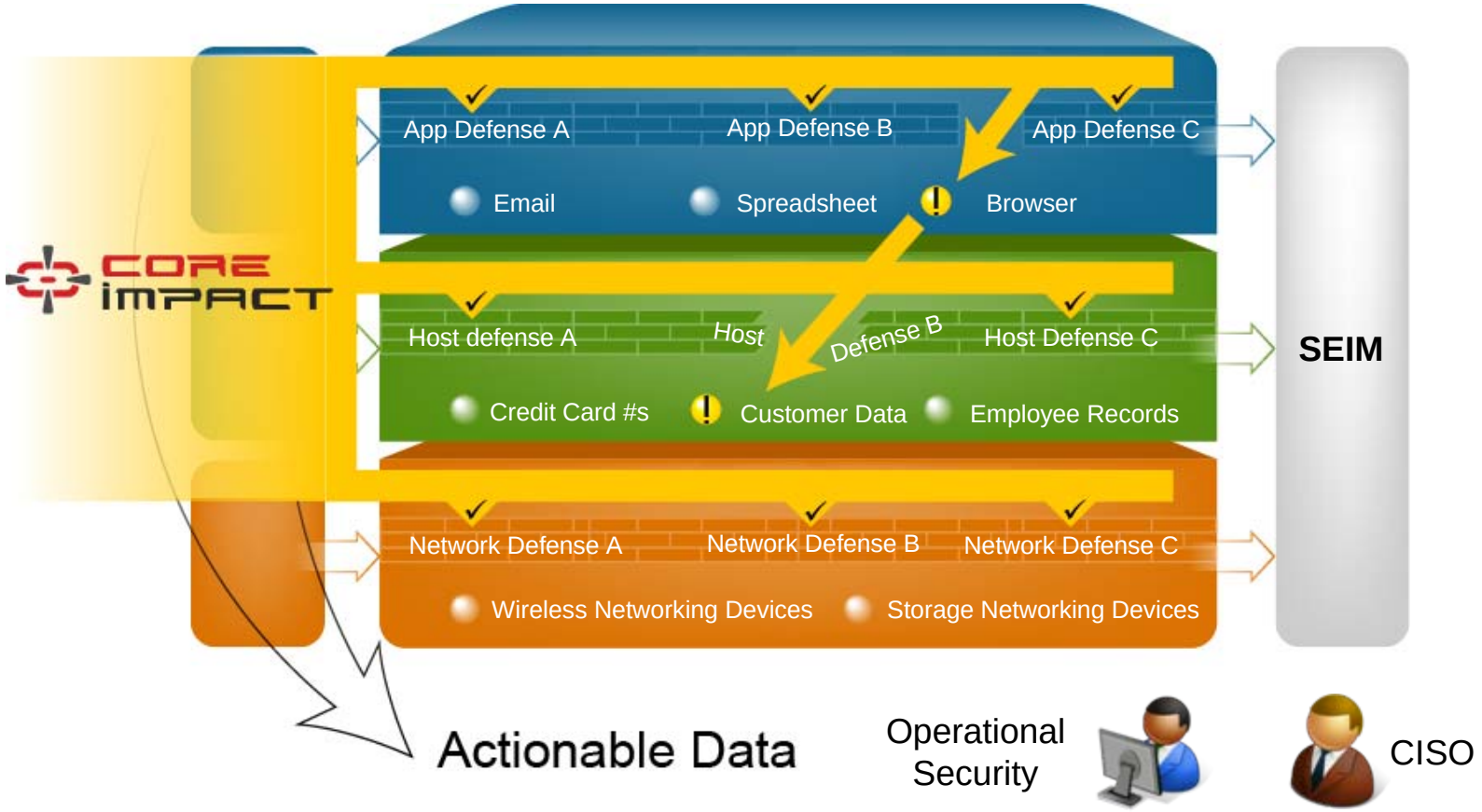
Comprehensive, Real-World Security Testing

CORE IMPACT provides comprehensive testing of your overall security posture.



Comprehensive, Real-World Security Testing

By identifying and validating the most critical, exploitable risks, IMPACT enables intelligent vulnerability remediation and helps to prioritize security initiatives.



Trusted Vulnerability Research & Leading Threat Expertise

The Knowledge Behind Our Products

- **CoreLabs (R&D)**
  - Filtering of known vulnerabilities for operational risks
  - Discovery of new vulnerabilities before criminals do
  - Collaboration with software vendors to remediate
  - Publishing of research papers and advisories
- **Core Security Consulting Services (Core SCS)**
  - Front-line risk assessment and custom analysis
  - Early identification of new threat vectors
  - Defining attack patterns & point solutions exposures
- **Core Engineering**
  - Commercial-Grade exploit creation
- **Core Products**
  - CORE IMPACT Pro
  - CORE IMPACT Essential

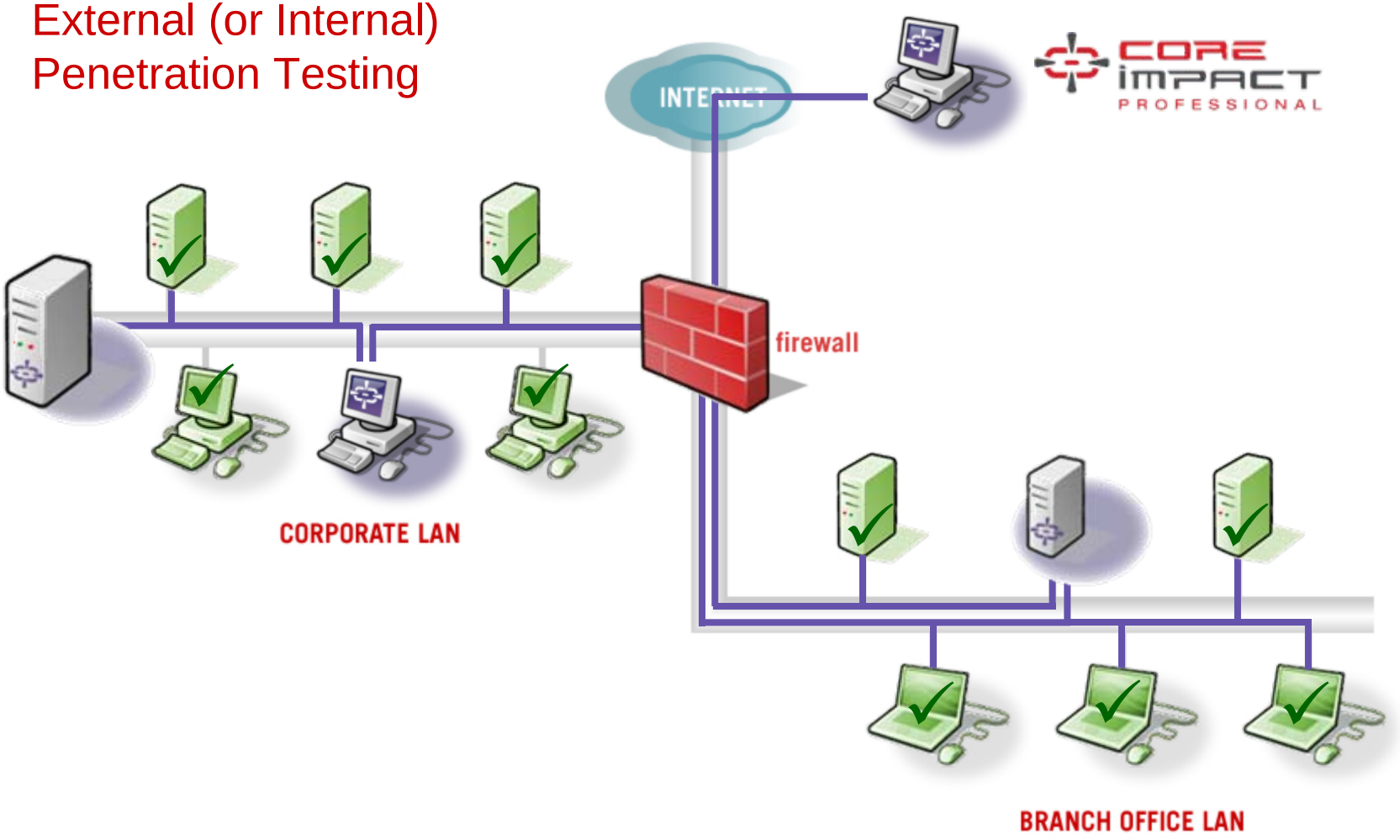
CORE IMPACT Pro Overview

- **Ideal for:**
  - Organizations with internal security professionals charged with conducting in-depth, comprehensive assessments of security readiness

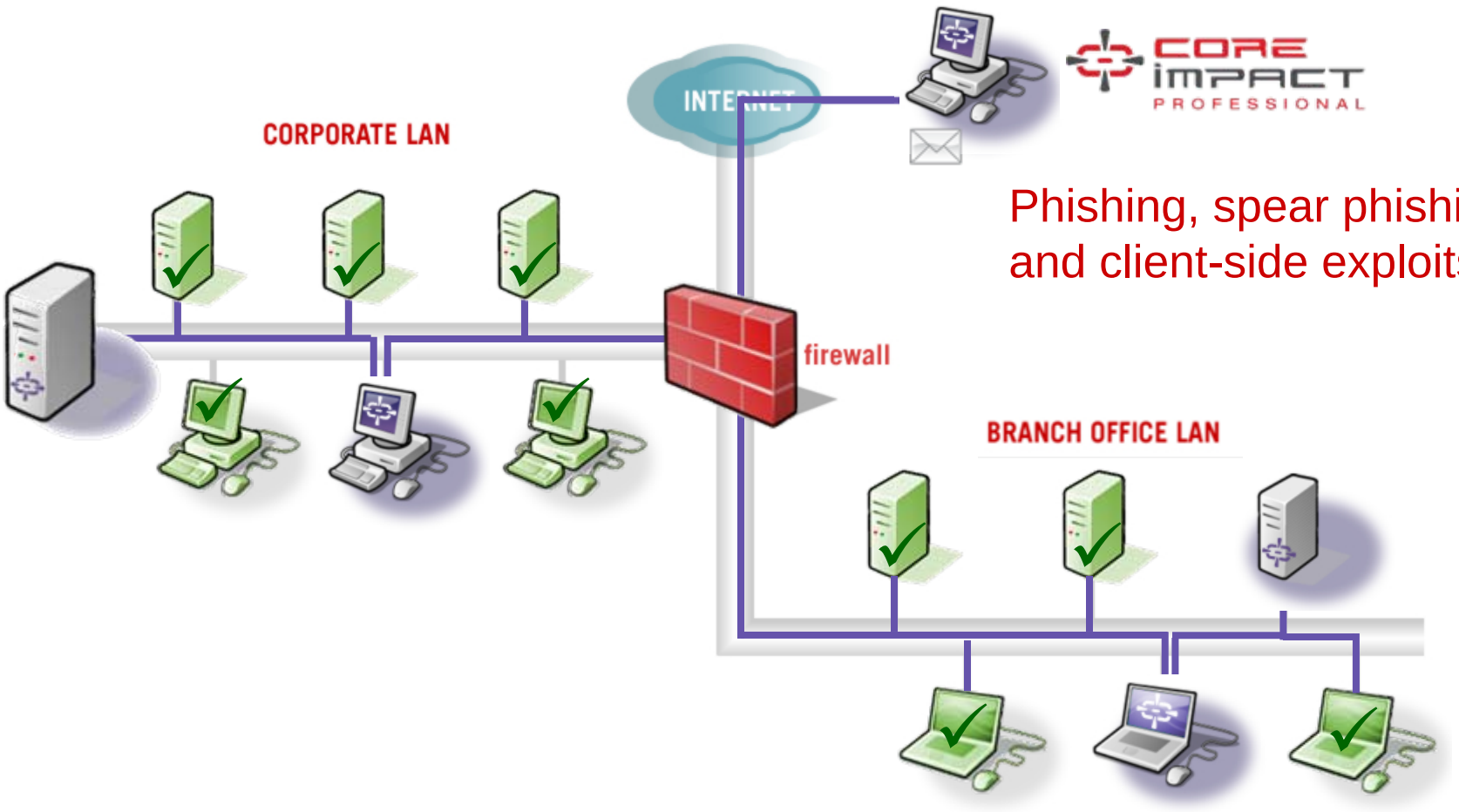
CORE IMPACT PROFESSIONAL

- **Testing coverage**
  - "Real-world," thorough assessment of network systems, endpoints, email users and web apps
  - Emulation of multistaged threats that pivot to backend systems
    - » replicates movement of threats between systems and across IT infrastructure layers
  - Provides a platform for testing against custom threats
- **Benefits**
  - Actionable data for reducing operational risk
  - Security testing that accounts for complex, multistaged attack behavior
  - Repeatable and safe testing processes
  - Automated RPT adds testing efficiencies / Manual modes offer full control
  - Full reporting of critical exposures and links to remediation info

External (or Internal) Penetration Testing

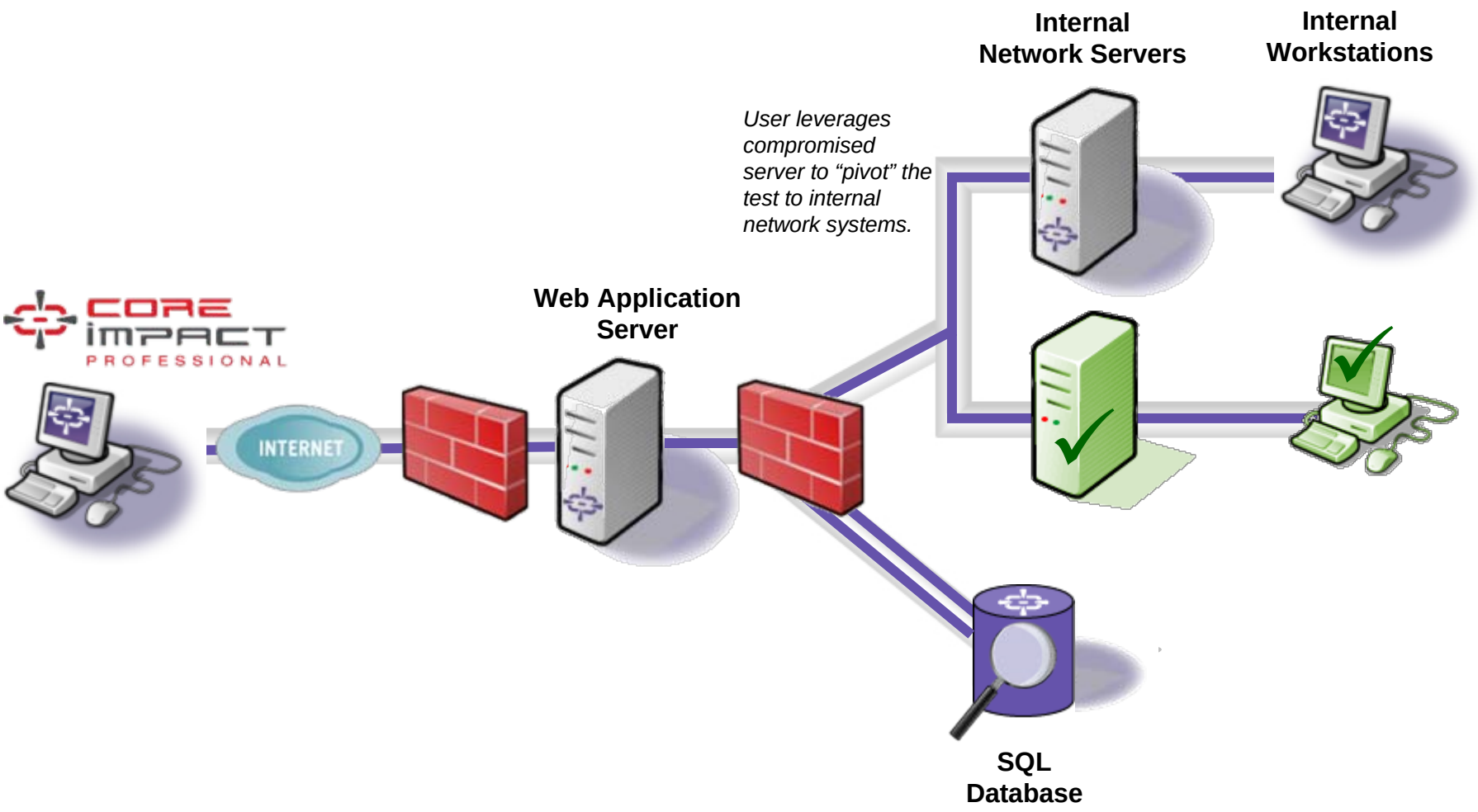


CORE IMPACT Pro: End-User Security Testing



Phishing, spear phishing and client-side exploits

CORE IMPACT Pro: Web App Security Testing



CORE IMPACT Essential Overview

- **Ideal for:**
  - Large organizations that need to equip branch staff with the ability to prioritize vulnerabilities between in-depth testing engagements by security personnel
  - SMBs where security is part of a broader IT role (e.g., no dedicated security staff)
- **Testing coverage**
  - Validating and filtering vulnerabilities identified by scanners
  - Identification and validation of critical network and endpoint vulnerabilities
    - » reveals initial entry points into an organization's IT infrastructure
- **Benefits**
  - Actionable data for reducing operational risk
  - Security posture verification with little time or effort required
  - Repeatable, safe and efficient testing processes
  - Full reporting of critical exposures and links to remediation info

Recognition

“Core’s smart dashboard, friendly UI, attack configuration wizards, and focused reports make penetration testing easier than ever ...”
- InfoWorld, January 2008

Security Software Product of the Year
- TechWorld, June 2007

“We have used IMPACT in SC Labs for two years and have found nothing else that even comes close”
- SC Magazine, December 2007

“CORE IMPACT 6.0 is an amazing tool to validate your security posture.”
- Information Security Magazine, January 16, 2007

“We have reviewed, tested, and played with many products and applications over the years, but none of them compare to CORE IMPACT.”
- informit.com, May 4, 2007

Wall Street Journal Technology and Innovation Award: Runner-Up, IT Security and Privacy
– September 2006

eWeek Excellence Awards: Vulnerability Assessment and Remediation – May 2006

“CORE IMPACT was a blast to test and a product I am certain would benefit organizations that choose to engage it.”
- ISSA, May 4, 2007

"After using IMPACT it seems obvious to us that manual penetration is obsolete."
- Federal Computing Week, May 2006